





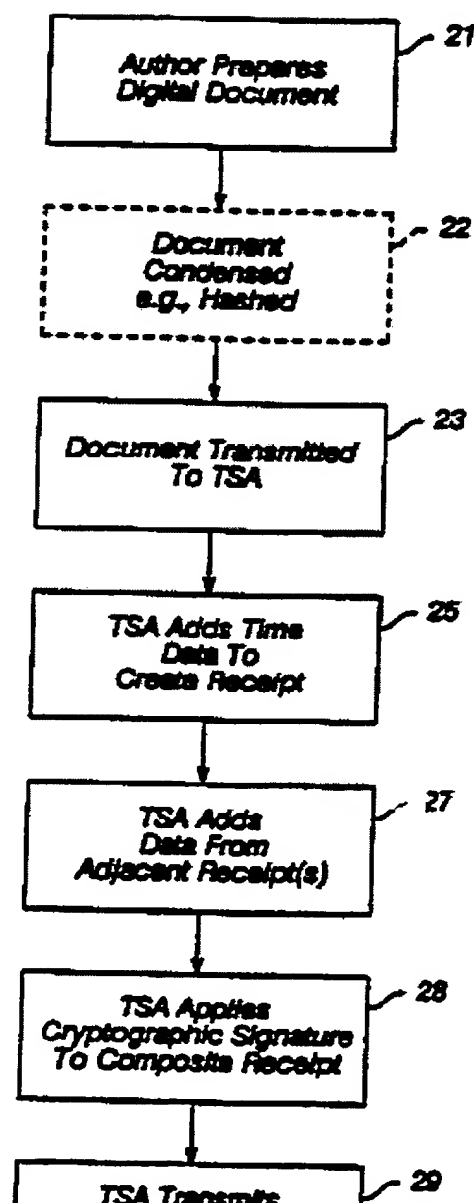


METHOD FOR SECURE TIME-STAMPING OF DIGITAL DOCUMENTS**Patent number:** WO9203000**Publication date:** 1992-02-20**Inventor:** HABER STUART ALAN (US); STORNETTA
WAKEFIELD SCOTT JR (US)**Applicant:** BELL COMMUNICATIONS RES (US)**Classification:****- International:** H04L9/00**- european:** H04L9/32T**Application number:** WO1991US05386 19910730**Priority number(s):** US19900561888 19900802; US19910666896 19910308**Also published as:** EP0541727 (A1)
 JP2002092220 (/)
 EP0541727 (A4)
 EP0541727 (B1)**Cited documents:** US4145568
 US4206315**Abstract of WO9203000**

A system for time-stamping a digital document is disclosed which protects the secrecy of the document text and provides a tamper-proof time seal establishing an author's claim to the temporal existence of the document. Initially the author prepares the document (21), which may then be condensed by a process such as hashing (22). Next, the document is transmitted to the Time Stamping Authority (23), which adds time data to create a receipt (25) and data from adjacent receipts (27). Thereafter, the Time Stamping Authority applies a cryptographic signature to the composite receipt (28), which is then transmitted to the author (29).



(19) 日本国特許庁 (J P)

(12) 公表特許公報 (A)

(11) 特許出願公表番号

特表平6-501571

第6部門第2区分

(43) 公表日 平成6年(1994)2月17日

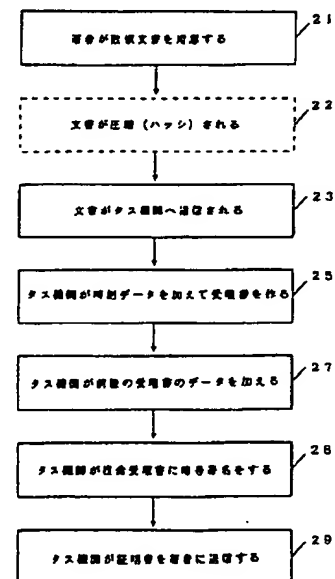
(51) Int. Cl. ³	識別記号	庁内整理番号	F I	
G 0 9 C 1/00		9194-5L		
H 0 4 L 9/32		7117-5K	H 0 4 L 9/00	A
審査請求 有 予備審査請求 有 (全 10 頁)				
(21) 出願番号	特願平3-516026	(71) 出願人	ベル コミュニケーションズ リサーチ インコーポレーテッド	
(86) (22) 出願日	平成3年(1991)7月30日		アメリカ合衆国、07039-2729 ニュージ ャージー州、リビングストン、ウエスト	
(85) 翻訳文提出日	平成5年(1993)2月2日		マウント プレザント アベニュー 290	
(86) 国際出願番号	P C T / U S 9 1 / 0 5 3 8 6	(72) 発明者	ハバー、スチュアート、アラン	
(87) 国際公開番号	W O 9 2 / 0 3 0 0 0		アメリカ合衆国、10003 ニューヨーク州、 ニューヨーク、アービン プレイス 22、 アパートメント 2 シー	
(87) 国際公開日	平成4年(1992)2月20日	(74) 代理人	弁理士 小林 孝次	
(31) 優先権主張番号	5 6 1, 8 8 8			
(32) 優先日	1990年8月2日			
(33) 優先権主張国	米国 (U S)			
(31) 優先権主張番号	6 6 6, 8 9 6			
(32) 優先日	1991年3月8日			
(33) 優先権主張国	米国 (U S)			

最終頁に続く

(54) 【発明の名称】 数値文書にタイムスタンプを確実に押す方法

(57) 【要約】

文字数字式やビデオやオーディオや絵のデータを含む、数値文書にタイムスタンプを押すシステムは文書テキストの秘密を守り、その文書が成立した時刻に対する著者の主張を確立する、不正変改の恐れのない時刻のシールを提供します。最初に、文書は一方方向性のハッシュ関数で一つの数字に圧縮され、これによって文書テキストの独自の表示を確定するかも知れません。本発明の一実施例ではこの数字はそれから外部機関に送信され、そこでその時の時刻が加えられて受理書が作られ、これが公開鍵署名法で機関によって証明されて、文書存在の証拠として著者に返されます。機関によるタイムスタンプに通謀による不正がないようにし、システムの信頼性を高めるために、受理書は他の同じ頃の受理書と結合され、かくして連続の時の流れの中の文書の位置を確定してから、機関によって証明されます。他の実施例では、タイムスタンプされる文書のハッシュ数の関数を独自の種として、これによる無作為選択によって複数の機関が指定されます。もう一つの実施例では、機関は受理書のデータにその時の記録連鎖証明書を加えてハッシュして受理書を



特許請求の範囲

証明します。ここでその時の記録連鎖証明書は前の受理書の夫々をその時々々の連鎖証明書と次々にハッシュした結果得られる数です。文書の内容を後で証明するには、機関の公開の鍵を使い、問題の文書の表示を使って証明の段階を繰り返して、証明書の真正であることが認証されます。問題の文書が原文書と同一である時だけ両方の証明書の数が一致します。

1. a) 数値文書の数値表示が制作者から外部機関へ送信され、
b) この外部機関がこの数値文書の数値表示の少なくとも一部分とその時の時刻の数値表示とを包含する受理書を作り、
c) この受理書がこの外部機関によって証明できる数値符号署名法によって証明されることを特徴とする数値文書にタイムスタンプを付与する方法。
2. 前記数値文書表示受理書が前記数値文書に決定関数法を適用して得られる数の数値表示の少なくとも一部分を包含する前記特許請求の範囲第1項記載の方法。
3. 前記数値数値表示が前記数値文書に一方方向ハッシュ法を適用して得られる前記特許請求の範囲第2項記載の方法。
4. 前記受理書が前記外部機関が受理した他の数値文書の少なくとも一つに特有な時刻表と数値文書表示を更に包含する前記特許請求の範囲第1項記載の方法。
5. 前記外部機関が予め定められた世界から、前記数値文書に決定関数法を適用して得られる数の数値表示の少なくとも一部分を覆として数値無作為発生機で無作為に、選ばれた前記特許請求の範囲第1項記載の方法。
6. 前記数値無作為発生機の程が前記数値文書に一方方向ハッシュ法を適用して得られる前記特許請求の範囲第5項記載の方法。
7. 前記数値無作為発生機によって選ばれた少なくとも一つの付加的な外部機関によっても同時にタイムスタンプ証明書が作られる前記特許請求の範囲第5項記載の方法。

8. 前記数値無作為発生機によって選ばれた少なくとも一つの付加的な外部機関によっても同時にタイムスタンプ証明書が作られ、夫々の付加的な外部機関の選択時の入力値は以前に作られた出力の数値表示に前記一方方向ハッシュ法を適用して得られる出力の数値表示の少なくとも一部分である。前記特許請求の範囲第7項記載の方法。

9. a) 一つのシリーズの文書の特定の数の数値表示を作り、
b) 前記特定文書表示と前記シリーズ中の前記特定文書の直前の文書に対する証明書記載連関数表示を包含する連関に対して決定関数法を適用して前記特定文書に対する証明書記載連関数表示を作ることを特徴とする一つのシリーズの数値文書の時刻的順序を証明する方法。

10. 前記シリーズの以後の文書の夫々に対して前記の段階を繰り返すことを更に包含する前記特許請求の範囲第9項記載の方法。

11. 前記文書表示の夫々が前記文書に決定関数法を適用して得られる前記特許請求の範囲第10項記載の方法。

12. 数値文書の数値表示を外部機関に送信し、前記外部機関がこの時の時刻の数値表示と前記数値文書の数値表示の少なくとも一部分を包含する受理書を作り、前記外部機関で前記受理書を証明する時、

- a) 前記受理書の数値表示を以前の証明書記載連関数の表示と連関して複合表示を作り、
- b) 前記複合表示に決定関数法を適用して前記受理書に対する証明書記載連関数を作る

ことによって前記受理書を証明することを特徴とする数値文書にタイムスタンプを付与する方法。

13. 前記外部機関がこれ迄のタイムスタンプ処理の証明書記載連関数を包含する記録を維持する前記特許請求の範囲第12項記載の数値文書にタイムスタンプを付与する方法。

14. 前記受理書に含まれる数値文書表示が前記数値文書に決定関数法を適用して得られる数の数値表示の少なくとも一部分を包含する前記特許請求の範囲第12項記載の数値文書にタイムスタンプを付与する方法。

15. 前記数値表示が前記数値文書に一方方向ハッシュ法を適用して得られる前記特許請求の範囲第14項記載の数値文書にタイムスタンプを付与する方法。

明細書

数値文書にタイムスタンプを確実に押す方法

発明の背景

文書が書かれた日付を立証し、問題の文書の内容が日付の押された原文書の内容と実際に同じであることを証明することが多くの場合に必要です。例えば、知的財産に関しては、ある人が発明の内容を最初に記録した日付を立証することは極めて重要です。発明の考えをタイムスタンプする普通の方法は、研究室の記録帳に自分の仕事を毎日書き込むことです。消せないように日付を書いて書き出した記録が記録帳の各ページに次々と書き込まれ、縦書き番号を打たれて綴じ込まれたページは記録を消さないように固定することを要します。記録の真正性は、一般に利害関係のない第三者によって定期的に検閲され証人として署名されることによって、更に高められます。何時考えたかということが後で証明されなければいけなくなった時、記録帳の物理的な内容と定められた記録の手順の両方が、少なくとも記録帳の証人の日付の時には考えが存在していたという事実を立証する効果的な証拠となります。

読むことのできるテキストの数値的な表示だけでなく、ビデオやオーディオや他のデータをも含む、電子文書が度々広く使われるようになって来て、このような文書の日付を確立する「記録帳」の概念の実行可能性が脅かされています。電子数値文書は極めて容易に改訂され、このような改訂は後に証拠を減らすので、ある文書が作られた日付を本当にその文書が示しているのか、又元のメッセージを今でも本当に表しているのかについて

ついて同等な証拠を提供しますが、このメッセージの受取人だけが、メッセージは受取った時刻以前に存在したことを知る事ができますから、この限界は今でもあります。しかし、このような受取はメッセージが存在した時刻の正確な証拠を全世界に提供はしません。受取ったメッセージに照準する受取人の証言はメッセージの内容とその存在の時刻についての証拠を提供しますが、このような証拠は電子数値文書の内容が、送信者または証人によって簡単に改訂できるという基本的な問題を抱えています。

従って、読者の文書が簡単に改訂できる数値形式で書かれる世界になるという予想は、このような文書の信頼性を確立する既存の手段を本質的に危うくします。数値文書の内容と時刻を確定し、少なくとも有形式文書の場合に現在認められている程度に、内容と時刻に対して直接的な証拠を提供することができるような立証のシステムが現在明白に必要とされています。

発明の概要

この発明は数値文書をタイムスタンプする方法において信頼できるシステムを作り、現在の記録帳の本来の機能の二つと同等のものを提供します。第一に、文書の内容とその存在のタイムスタンプは、文書の数値データに消えないように綴じ込まれ、これによって出来たタイムスタンプされたデータのいかなる部分も、改訂が明白とならないように改訂することは不可能であります。このように、文書のテキストの状態はタイムスタンプの瞬間に確定されます。第二に、数値文書がスタンプされた時刻は、虚偽の時刻の表現を綴じ込むことを防ぎ、数値的に「証人として」署名する手順で確認されます。基本的に、この方法はタイムスタンプの運用のコントロールを著者から独立機関へと移し、其の時刻以外のス

は、信頼できる証拠は限られています。同じ理由で、立証する署名の信頼性についても重大な懸念が起きて来ます。数値文書の内容の改訂を作さない結果的な手段がないと、システムの信頼性が基本的に欠けていることは電子文書の有効性がもつと広く適用されることを妨げます。

現在でも、電子文書の送信を確証する若干の手段があります。しかし、実際にはこのような手段は両方向の通信に限られます。即ち、このような通信では、送信者は送信される文書の元来の内容と発信者を受信者に立証しようと本質的に望みます。例えば、「秘密の鍵」を使う暗号化は長い間、限られた数の、お互いに知合っていて暗号を解く鍵を知っている個人の間で、メッセージの送信に使われてきました。メッセージを暗号にすることは不正検閲を防ぎ、秘密の鍵を使うと送信されたメッセージの「平文」が得られると言う事実が、メッセージは決まったグループの一員が送信したものである証拠となります。しかし、メッセージを書いた時刻は間接的に、受信者が受取った時刻より後ではないと、証明されるに過ぎません。それで、この方法は限られない世界で使われて役に立つタイムスタンプの証拠を提供しません。

もつと広く適用される立証通信法、即ち「公開の鍵」を使う暗号化が、ディフィーとヘルマン（「暗号化の新しい方向」、IEEE 情報理論雑誌、第17-22号、昭和51年11月、644-654ページ）によって記述され、その後リベスト等によって、昭和58年9月20日付のアメリカ合衆国特許4,405,829号で実行された。この方法は利用者の世界を、公表された名前以外ではお互いに未知の、実質上限定されない数のシステム加入者に拡大しましたが、立証できる通信は依然として両方向のものでした。送信者の秘密の鍵で暗号化されたメッセージの公開の鍵での暗号化を伴うもののような、公開の鍵の「署名」は、限定されない世界のどのメンバーにもメッセージの送信者が誰かに

スタンプをするよう機能に影響を及ぼす能力を著者から取り上げます。

この発明の方法は、文書の書きが送信網の中に沢山散らばっていると仮定します。このような著者は個人、会社、会社の部門等で、夫々が区別され、識別番号等で特定できる。著者世界の一員です。この発明の一つの実施例では、この世界はタイムスタンプ機関（タス機関）の依頼人で構成されます。もう一つの実施例では、散らばった著者の夫々がこの世界の他のメンバーの為にタイムスタンプのサービスを行う機関であります。

一般の運用においては、図面の第1図に示されるように、この方法では、著者が広く文字、数字、音声、図画の表示を含む数値文書を作成し、この文書を、好ましくは圧縮した形で、タス機関へ送信します。タス機関は受理した時刻を表す数値データを加えて文書にタイムスタンプし、この文書にその機関の署名を入れて暗号化し、できた文書即ち原文書の存在時刻証明書を著者に送信し、著者はこのような存在を証明することが必要になる時の為に保管します。他の方法では、タス機関は受理した時刻を表す数値データを加えて文書にタイムスタンプし、受取書を作ります。これまでの受取書を暗号化されたものにこの受取書を送信し、この複合文書から以下に詳述する決定関数を使って新しい数値文書を作ります。これによってできた数値文書を時刻その他の数値データと一緒にして証明書を作ります。

タス機関への送信中に秘密文書の情報が盗取されるのを防ぐために、また全文書の送信に要する数値帯域幅を減らすために、著者は場合によっては数値文書の一種子を決定関数を使って数値のサイズを大幅に圧縮して独自の値に立換えるかも知れません。決定関数としては、例えば専門分野では「一方方向ハッシュ関数」として知られる多数のアルゴリズムのどの一つでも使えます。ハッシュ関数のこのような応用は、例えばダムガードによって文書

署名法における安全改良の基盤の中で述べられています（「衝突のないハッシュ関数と公開鍵を使う署名法」、暗号学の進歩—ユーロクリプト1987、スプリンガー・フェルラーク、LNC S、1988、第304巻、203-217ページ）。しかし、この発明の応用では、ハッシング法に典型的な「一方」性はもう一つの目的に叶います。すなわち、タス機関がタイムスタンプを押したり、文書を遠隔証明書に送込んだ後では、文書は密かに改竄されることはできないという保証を提供します。

ハッシング関数は丁度このような保証を提供します。というのは、署名の原素や合成距離受理書のような文書がハッシュされる時に元の内容の代表的な「指紋」が作られ、これから元の文書を復元することは、ほとんど不可能です。それゆえに、タイムスタンプされた文書は署名の改訂版に適用することはできません。なぜならば、原文書の内容の改変は、たとえ一語または数語データのビットでも、違った文書となり、全く違った指紋値のものにハッシュするからです。代表的なハッシュ値から文書を復元することはできませんが、それにもかかわらず、原文書と主張されているものはこのタイムスタンプ手順で証明されます。というのは原文書表示の真のコピーを包含する受理書は、元のハッシング法を使えば署名の持っている証明書に含まれている、元の数字または同じ距離値に何時でもハッシュするという事実があるからです。

この手順では現在あるどんな決定関数でも使えますが、たとえば、リベスト（「MD4」メッセージ・ダイジェスト・アルゴリズム」、暗号学の進歩—ユーロクリプト1990、スプリンガー・フェルラーク、LNC S、近刊予定）が述べているような一方向性ハッシュ関数を引用してここに組み入れて置きます。この発明の実用においては、かようなハッシング操作は場合によっては署名によって通信中の防竄という著しい利点のためになされます。文書

が暗号文でない形で受理された場合にはタス機関がハッシングするかも知れません。文書の内容と送込んだ時刻のデータが改竄されないようにどのように確定されても、このシステムの信頼性を増すためには、未定世界のメンバーに対して、受理書は、署名ではなく、実際にタス機関によって作られ、示された時刻は正しく、例えば署名と共有したタス機関が許容的に公表したものでないという証明が提供されています。

第一の局面に対しては、タス機関は、前述の公開鍵の方法のような、検証できる署名法を用いて、署名へ送信する前にタイムスタンプを押したと証明します。後で、タス機関の公開鍵での署名の検証は、署名と世界全体に対して、証明書はタス機関が作ったものであると証明します。しかしながら、タイムスタンプ自身の真実性の証明は、以下に述べるこの発明の他の部分に依存します。

別の方法では、タス機関は、新しく受理したものを一つ一つその時点までの距離に付け加え、この値を表示に決定関数を用い、即ちハッシングを行い、新しい距離を作ると、順次にタイムスタンプした時刻の距離を維持します。この距離はハッシング過程によって作られた値で、これが署名に与えられる受理書または証明書に記されて、そこに示されるタイムスタンプを証明するのに役立ちます。後で証明書の検証をするのには、署名の時刻受理書とタス機関の記録にあるその直前の距離の値の組合わせに再度ハッシュを行います。その結果署名の証明書に記録の距離値が出れば、署名と全世界に対してその証明書はタス機関で作られたものであると証明します。この結果はまたタイムスタンプの真実性をも証明します。というのは元の受理書に記録の値で元の距離を使わなければ、ハッシング関数によって元の証明書に記録の距離値を作ることはできないからです。

第2図に一般的に書かれているような、この手順の一つの実施例では、署名の世界からタ

ス機関の距離へと比較的に距離な文書の流れを利用します。天々の処理した文書D₀に対してタス機関はタイムスタンプ受理書を発行し、これには、たとえば、距離受理番号F₀、署名A₀の距離番号ID₀等による距離、文書のハッシュH₀、その時の時刻t₀が含まれます。タス機関はこの他に、直接に処理した署名A₀の文書D₀の受理データも含め、これによって文書D₀のタイムスタンプは独立に確立された前の受理時刻t₀によって「過去」の方向に限定されます。同様に、次に受理した文書D₁の受理データも、文書D₀のタイムスタンプを「将来」の方向に限定するために、含められます。複合受理書は今や3つ、あるいは希望によってはそれ以上の、連続したタイムスタンプ受理書の時刻のデータを含み、あるいはそれらの距離部分を含み、タス機関の暗号署名で証明されて、署名A₀に送信されます。同様にして、D₀とD₁の距離表示を含む証明書が署名A₁に送信されます。このようにして、タス機関によって出されたタイムスタンプ証明書の文々は連続した時間の中で確定され、交付された多数の連続した証明書を原素すれば署名が通ってれば直ちに判るので、タス機関はどれも集めて発行することはできません。時の流れでの文書のこのような順次の確定は非常に効果的なので、タス機関の署名は実際には必要ありません。

第3図に一般的に書かれているような、この手順の第二の実施例では、たとえばタイムスタンプの手順を利用する多数の署名といった、広い世界の中にタイムスタンプの仕事を実行し、タス機関を管理の目的に使ってもよく、あるいは拡張する署名は直接選択したタイムスタンプする署名と距離と距離してもよいわけです。いづれにしても、署名とタス機関の距離でタイムスタンプが文書に押されたのではないという保証が上記の様に必要で、これは少なくとも距離の世界のある部分は実証しようとする署名に買収されないか、そのような署名に距離の脅威をもちたすという合理的な脅威と、特定の文書をタイ

ムスタンプする機関はこの世界から全く無作為に選ばれたという事実の両方で満たされます。署名が署名の自身の選択で共有しそうな機関を選ぶことが出来ないことは、基間的な時刻の急造の可能性を事実上除きます。

この世界の個人のメンバーの中から予定数の機関を選ぶのは、インバグリアツォ、レビンとルビー（「一方向性関数による類似無作為発生」、第21回STOC会議、12-24ページ、ACM、1989）によって与えられた型の類似無作為発生機によってです。これに対する最初の値はタイムスタンプされる文書の、ハッシュのような、決定関数であります。値の入力として文書のハッシュ値のこのような関数を与えられると、条件を満たす類似無作為発生機は一群の機関の距離番号を出力します。この機関の選択は実際上予選で必ず無作為です。

機関が選ばれたと、タイムスタンプは前述のように行われますが、天々の機関は創性的に受理時刻のデータを受信した文書に付け加え、その結果できたタイムスタンプした別の受理書を機関固有の証明可能な暗号署名で証明し、証明書を署名に送信します。この送信は申請した署名に距離の場合もあり、管理するタス機関を離れる場合もあり、後者の場合にはタス機関が更に証明を付け加えるかも知れません。署名をするという機関と公表された署名の距離番号は、実際に類似無作為発生機で選択された機関を利用したことの証明を与えます。本発明の分布した機関を使う実施例は受理書を遠隔する方法に比べて、タイムスタンプ証明書がより早く発行され、また文書の署名の数での証明は他の署名の証明書が入手できるかどうかにかわり依存しない利点があります。

第4図に示される別の実施例では、タス機関が作るタイムスタンプ受理書に、たとえば受理時刻と番号F₀、署名の距離、たとえば距離番号ID₀等、文書の距離表示、たとえばハッシュH₀、とその時刻t₀を含めます。この後タス機関は受理書のこれらのデータ（また

はその代換的な任意の部分)を、その直前に処理した、著者A₀の文書D₀の証明書記録部値C₀に包含し、これによって文書D₀のタイムスタンプを、値C₀に確定された時の受信時刻t₀で確定します。

この複合データの数列 {r₀, ID₀, H₀, t₀, C₀} はその後ハッシュされて新しい記録部値C₁となり、これが処理番号r₁とともにタイムスタンプの記録に入れられ、またタイムスタンプ受信データとともに証明書記録部値としてA₁に送信されます。同様に、C₁と書頭D₁の受信者のタイムスタンプ部値をハッシュして得られる証明部値が著者A₁に送信されます。このようにして、タイムスタンプが出したタイムスタンプを付した証明部値の次々は連続した時の中に確定され、タイムスタンプは集って作ることは出来ません。何故ならば、前の証明部とハッシュして証明書記録部値を再生しようとすれば矛盾を示すからです。

第5図に示されるような、この発明のより一般的な運用においては、特定の文書の表示、すなわちハッシュは直前の文書の証明書記録部値と異に算出され、この直前表示の決定部数表示、たとえばやはりハッシュ、が次に作られて、この特定の文書の記録上の記録部として保持されます。この増大して行くシリーズの以後の次々の文書は同様に処理されて記録を拡張し、この記録自身がこのシリーズの中で、もっと広く見れば連続した時の中で、このような文書の次々が占める位置の位置できる証明となります。本発明のこの実施例は、たとえば記録がその記録上の数値の文書や記録の順序や連続性を互に証明できる位置でする方法を提供します。

本発明の手段の別の態様では、著者の記録の中である時間の内に、これは活動の程度によりますがたとえば一日とかそれ以上の間に、作られた(許ましくはハッシュしたりその他の表示の形の)文書の展開をハッシュして、タイムスタンプと証明に付帯的な単一の文書とし

発明の記述

本発明の実施例を適用した以下の例で、含まれた手順を更に説明します。説明の便宜上、述べた決定部数は上記のリストによって記述された md4 ハッシュ法で、また証明できる署名法はディフィーとヘルマンによって示唆されリスト等によってアメリカ合衆国特許4,405,829号で実行された公開の方法です。タイムスタンプが実際に適用される手に入る方法の中のどれでも良いです。どのような方法が用いられても、何をどの証明使ったかという記録は、受信証明書を後で確認するために維持されなければなりません。更に、手順の説明を簡潔にするためと以下に述べるそれ以外の理由の為に、数字の代換的な部分だけを用います。

第2図に示される本発明の受信部値の実施例を最初に考えましょう。この手順はどの様な長さの文書にも使えますが、以下の適切な引用は、ある著者が段階21で書いてタイムスタンプを希望する文書D₀を充分に代換するものです。

Time's glory is to cast contending kings,
To unmask falsehood, and bring truth to light,
To stamp the seal of time in aged things,
To wake the sorn, and sentinel the night,
To wring the stranger till he render right;

The Rape of Lucrece

破線で囲まれた任意段階22で、この文書はmd4 算法によって標準の128ビットの値H₀にハッシュされますが、この数H₀は16進法では

a f 6 d f d c d 8 3 3 f 3 a 4 3 d 4 5 1 5 a 9 f b 5 c e 3 9 1 5

となります。1000人からなる著者世界の中でシステム部番号ID₀が172である

ます。また、偶然然作あ発生値の値は、その文書によるだけでなく、特定の時刻や時に受信部が与えられた文書にもよるかもしれません。別の方法では、一つの記録のなかで信託された人が、常態する「外部の」機関として、この手順を使ってその記録の文書の証明部値の記録を維持し、定期的にその時々の高層証明書をタイムスタンプに送信します。このようにして、ある記録の記録上の記録の順序が、記録の中でも、また外部的にはタイムスタンプを通じて、確定されます。

また、手取実施例の実行は、原文書表示の受信・ハッシュ・記録、タイムスタンプ押印、証明書記録部値の計算と記録、受信証明書の発行という諸段階を連続行い、単一の電算機のプログラムで直ちに自動化されます。

図面

本発明の説明には以下の図面を用います：

第1図は本発明による文書タイムスタンプの一般手順の流れ図です。

第2図はこの手順の特定の実施例の流れ図です。

第3図はこの手順のもう一つの特定の実施例の流れ図です。

第4図はタイムスタンプ手順の他の実施例の流れ図です。

第5図は本発明による一般記録手順の流れ図です。

著者A₀がこの記録番号を付けた文書を段階23でメッセージ(ID₀, H₀)：

1 7 2, a f 6 d f d c d 8 3 3 f 3 a 4 3 d 4 5 1 5 a 9 f b 5 c e 3 9 1 5

としてシステムのタイムスタンプに、この文書をタイムスタンプする装置として、送信します。

タイムスタンプは、段階25で、たとえば132という受信部値番号r₀と、その時の時刻t₀の値を付け加えて、文書D₀の受信部を発行します。この時刻の値は、著者A₀ができたタイムスタンプ証明書を容易に読めるようにするために、電算機の時計の時刻の標準32ビット表示と文章による伝送を、たとえば1990年3月10日グリニッジ平均時16:37:41のように与えるかもしれません。そうすると受信部は数列 {r₀, t₀, ID₀, H₀} を包含します。

この点で、表示セグメントの数のサイズを前述のように減らすということを更に考えることが必要であります。リスト等によってアメリカ合衆国特許4,405,829号で記述されたように、この例で使われる符号公開鍵法(この分野では一般に「RSA」署名法として知られています)は、長いメッセージを、一つ一つが暗号化暗号鍵を越えない数で長されるブロックに分割することが必要です。次々のこのブロックはこのRSA法で署名され、送信された後またアセンブルされます。それゆえに、RSA法で証明する最終の受信部数列が単一のブロックであることを維持しながら、この例で長大な大きな数の数nを使えるためには、受信部数列の次々の要素は代表的な8ビットに減らされますが、長すぎる数値の場合には普通は最後の8ビットとなり、このビットは16進法では2つのヘキサデシマルの字となります。それで、たとえば、128ビットの文書ハッシュH₀は最後の8ビット、すなわち0001 0101で表され、これは16進法では15と書かれます。同様に、ID₀の172は1010 1100で、16進法ではacとなります。

す。実際の計算を行わないで、時刻表示 t_{i-1} は51と表示されると仮定しましょう。受理番号132は84と表示されます。この点で受信者の数列 $(r_{i-1}, t_{i-1}, ID_{i-1}, H_{i-1})$ は8451a c 15となります。

ここで、直前の文書 D_{i-1} はタス機関によって1990年3月10日16:32:30に (t_{i-1}) の表示は64)に申請

201, d2d67232a81d816f7b87d014dc575174

として処理されたと仮定しましょう。段階27でタス機関はこれらのデータを D_i に対する受信者数列に加えて、15進数の表示、8451a c 15840974、を作ります。この受信者 R_i は今や D_i に対する時刻と、それ以前には著者 A_i が D_i が存在したと主張できない時刻 t_{i-1} を確定するデータを含みます。 A_i に対するこの確定は、前の著者 A_{i-1} が時刻証明書 c_{i-1} を保持し、それが t_{i-1} は著者 A_{i-2} の証明書にあるリンクされた時刻のデータ t_{i-2} の以後であると確定し、というように、証明が必要なだけ続くからです。

タス機関が文書 D_i の受信者を実際に発行したことを確立するために、段階28でタス機関は公開鍵暗号署名法で署名をし、段階29でこの受信者は著者 A_i に送信されて受信証明書または証明書 c_i となります。上のようにして得られたデータを使い、またタス機関は十進数でRSA署名セット

$\langle n, e \rangle = \langle 4320677821428109, 191 \rangle$ (公開)
 $\langle n, d \rangle = \langle 4320677821428109, 29403802422449791 \rangle$ (秘密)

を持つとすれば、 R_{i-1} 、8451a c 15840974、に対する署名付き証明書は

$R^e \bmod n = 39894704664774392$

前例の例と同じく、著者は文書をタス機関へ、普通ハッシュした形で、署名番号を付けた申請として送信します：

172, ef6dfdc0833f3a43d4515a9fb5ce3915

タス機関は、段階33で、この文書ハッシュ数列を最初の証人の署名番号を作る際として使い、段階35で、選択法

$ID = [md4(\text{書})] \bmod (\text{世界の大きさ})$

によって選びます。作られた値ハッシュ：

26f54aae92511dbb5e06e7a2de6e0f0f

は128ビットの数を表し、その $\bmod 1000$ が487で、これが最初に選ばれた証人のIDです。次の証人も同様にして選ばれ、この種のハッシュ表示を第2の選択の計算に使って

882653ee04d16b1f0d604883aa27300b

を得ますが、この $\bmod 1000$ は571で、これが第2の証人のIDです。この計算を繰り返して、前の種のハッシュを種に使うと最後の証人を598として選びますが、これは2fa8768ef3532f15a40acf1341902c1e $\bmod 1000$ です。

段階37で、タス機関は最初の申請書の写しをこれら3人の証人のそれぞれに送り、段階38で、証人は各個人その時の時刻のステートメントとIDを加え、こうしてできた受信者にRSA暗号署名法で署名して証明し、段階39で証明書を直接著者にまたはタス機関

と計算されるでしょう。著者 A_i がこの証明書 c_i と R_i の文章のステートメントを受取った時、タス機関の公開鍵を用いて

$c_i^e \bmod n = R_i$

となることから、 R_i は実際に文書のハッシュ H_i を表示するデータを含んでいると確認され、 c_i が正確であると直ちに確認されます。

この簡単な1リンクの例の手順で作られた証明書は文書 D_i のデータで時刻を確定されるので、著者 A_{i-1} に対して、文書 D_{i-1} は文書 D_i の存在のみかなり前に時刻を遅らせたのではないという信頼できる証拠を提供します。 A_i の証明書が以後に処理された文書 D_{i+1} からのデータを加えて拡大された時、この証明書は同様に体系的に確定され、 A_i が主張するタイムスタンプを立証します。同じ効果を得る別法としては、 A_i に A_{i-1} の名を教え、 A_i はその著者から1リンク証明書 c_{i-1} が資源 H_i を含むことを確認できます。この手順は改良させて、任意の数の著者のデータを含む受信証明書を発行するようにすることもでき、追加する毎に信頼がないという保証の度合いが高まります。

第3圖に示される本発明の別の実施例は著者世界の中から無作為に選ばれたメンバーがタス機関（または証人）となり、すなわち「分散信託」の手順ですが、これは以下のように行われます。実際の運用ではこれらの数はそんなにばらばらに確定されないのですが、この例では、世界は1000人の著者を含み、そのIDは0でない999で、タイムスタンプの真実性を確立するには3人の証人がいれば充分と仮定しましょう。また、この例ではタス機関のサービスを定める前記の改良が実行されています。前の例で用いられたハッシュ関数、md4、がここでも、任意の段階32で、著者世界から3人の証人を無作為に選ぶに選択する種をまく決定文書関数の一例として用いられています。

を通じて送信します。後の場合には、タス機関は証明書を一つのファイルにアセンブルして著者に送るかも知れません。証人の選択に当たって無作為発生を使うことは個人的な選択を防ぐという事実のために、著者は非暴力的な証人がタイムスタンプ証明の前に虚偽の時刻の記入を計算するために選択しようとする危険を避けられます。手順の別法として、著者が直接証人に申請することが許される場合、問題の文書自身が本質的に誰となる証人の無作為選択により、著者が文書を知人で暴力的な証人に向けようとする試みを難しくします。できた一冊の証明書は、前述のように署名確認をして、安心して後の証明に使えます。

図面第4圖の段階41のように、タイムスタンプ手順での遠隔証明書の作成は、著者 A_i が数個文書を準備することから始まります。前述のように、この数個文書は文字数字式テキスト、ビデオ、オーディオ、または確定したデータの他の形のものの数個的な形または表示であるかもしれません。この手順はどのような長さの文書に対しても用いられますが、以下の引用はタイムスタンプしたい文書 D_i を充分に代表します：

...the idea is which affirmation of the world and ethics are contained side by side ... the ethical acceptance of the world and of life, together with the ideals of civilization contained in this concept ... Truth has no special time of its own. Its hour is now -- always.

Schweitzer

著者が希望すれば、文書 D_i は安全と通信に必要な暗号幅を縮らすために、例えばmd4法で圧縮されます。段階で図まれた任意の段階42で示されるように、文書は第4の128ビットの形の値 H_i にハッシュされます。これは16進数で

e2ef3ea60df10cb621c4fb3f8dc34c7

持表平6-501571 (7)

となります。この点で留意しておきますが、この例で用いられる16進法やその他の数値表示は本発明の実施に決定的ではありません。すなわち、与えられた手順によって選ばれたこれらの値のどの部分もまたは他の表示も同様に作用します。

1000人の書き手の中で記録番号ID_nが634である書き手A_nが、段階43でシステムのタイムスタンプに、以下の記録メッセージ(ID_n, H_n)で、文書にタイムスタンプを押すよう要請し、文書を送信します:

634, ee2ef3ee60df10cb621c4fb3f8dc34c7

段階44で、タイムスタンプは、受理処理番号r_n、例えば1328、とその時の時刻t_nの表示を加えて文書D_nの受理番号を作ります。この時刻の表示は電算機の時計の時刻の標準2進表示かも知れず、または最終的なタイムスタンプ証明書が容易に読めるように、単に文章の表示で、例えば1991年3月6日グリニジ平均時19:48:28であるかも知れません。この時、受理番号は数対(r_n, t_n, ID_n, H_n)を包含し、これは

1328, 194628GMT06MAR91, 634,
ee2ef3ee60df10cb621c4fb3f8dc34c7

となります。

本発明によれば、この時のタイムスタンプの記録は、例えば、その時の記録番号と夫々の受理番号を次々とハッシュしてできた値の形で、以前の受理処理過程の連鎖を含みます。かくして、この連鎖記録は以下のようにしてできたものです。最初の処理(r_n=1)では受理番号は初値。すなわちタイムスタンプの記録のハッシュと共にハッシュされて最初の連鎖値c₁を作り、これが最初の処理の証明書の値として使われます。次の処理では、受理番号はc₁と連鎖され、

日付: 1991年3月6日
証明書数: 46f7d75f0fbce95e96fc38472ae28ca1

この手順はタイムスタンプによって以後のタイムスタンプ更新の順序繰り返されます。A_{n-1}からの次の要請がハッシュされた形H_{n-1}の文書

201, 882653ee04d511dbb5e06883ae27300b

で1991年3月6日グリニジ平均時19:57:52に受信されたとなると、複合連鎖は

46f7d75f0fbce95e96fc38472ae28ca1,
1329, 195752GMT06MAR1991, 201,
882653ee04d511dbb5e06883ae27300b

となり、A_{n-1}に送信される証明書は

処理番号: 1329
依頼人記録番号: 201
時刻: 19:57:52グリニジ平均時
日付: 1991年3月6日
証明書数: d9bb1b11d58bb09c2763e7915fbb83ad
となります。

持表、書き手A_{n-1}が文書D_{n-1}はタイムスタンプによって1991年3月6日19:57:52に受理されたことを証明しようと思えば、タイムスタンプの記録が読まれ、直前に処理された1328の連鎖受理番号c₁:

それがハッシュされて第2の証明書記録連鎖値c₂を作り、タイムスタンプのタイムスタンプ更新の連鎖を過ぎてこれが続きます。

現在の例の直前に文書D_{n-1}がタイムスタンプによって、第1327番目の受理番号として処理されて、証明書記録連鎖値c_{n-1}

26f54eae92516b1f0d6047c2de6e0fcf

を作ったと仮定しましょう。手順の段階45で、タイムスタンプはこの値とD_nの受理番号を連鎖して

26f54eae92516b1f0d6047c2de6e0fcf,
1328, 194628GMT06MAR91, 634,
ee2ef3ee60df10cb621c4fb3f8dc34c7

を作ります。この複合表示が、段階46で、タイムスタンプにハッシュされて、新しい証明書記録連鎖値c_nとして

46f7d75f0fbce95e96fc38472ae28ca1

を作ります。

この後タイムスタンプはこの値とその記録に加えて、段階47で書き手A_nにタイムスタンプ証明書を送信します。これには以下の証明書記録連鎖値もふくまれます:

処理番号: 1328
依頼人記録番号: 634
時刻: 19:48:28グリニジ平均時

46f7d75f0fbce95e96fc38472ae28ca1

が得られます。証明しようとする文書はタイムスタンプに送信された時の形、即ちハッシュに記録され、この値がc₁やその他のA_{n-1}の証明書に記録のデータと連鎖されます。関連の文書が本物であれば、複合表示は

46f7d75f0fbce95e96fc38472ae28ca1,
1329, 195752GMT06MAR1991, 201,
882653ee04d511dbb5e06883ae27300b

となり、これをハッシュすると正しい証明書記録連鎖値

d9bb1b11d58bb09c2763e7915fbb83ad

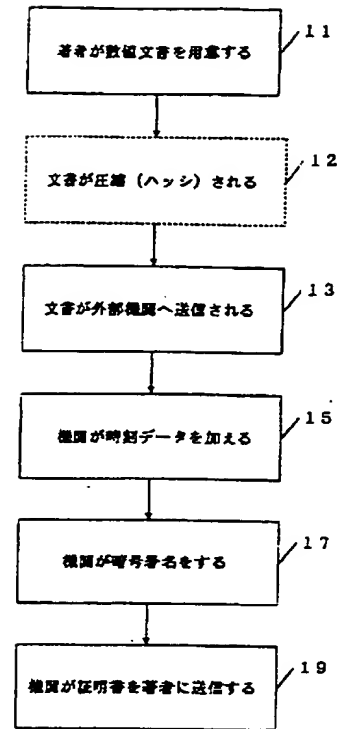
となって、関連の文書はD_{n-1}であることが証明されます。さもないれば、改訂された文書はハッシュされると違った値になり、これを要請として含む複合表示をハッシュしたものは、処理番号1329の証明書に記録の値と違った証明書記録連鎖値となります。

もしもつと証明が必要ならば、例えば文書を改訂した後でc_{n-1}も改訂したのではないかというような時には、タイムスタンプの記録から記録されるA_nの証明書と提出された、即ちハッシュした文書が使われて、その後の、問題となっている証明書c_{n-1}を再計算します。もしその値が正しければD_{n-1}は証明されました。別法としては、証明書c_{n-1}は、A_{n-2}の証明書値と提出された文書から次の証明書記録連鎖値c_{n-2}を再計算して証明されます。というのは、もしc_{n-1}がD_{n-2}を処理番号1330で処理した時のものと同じでなければ、後の文書を改訂してc_{n-2}と同じ値を得ようすることは不可能だからです。

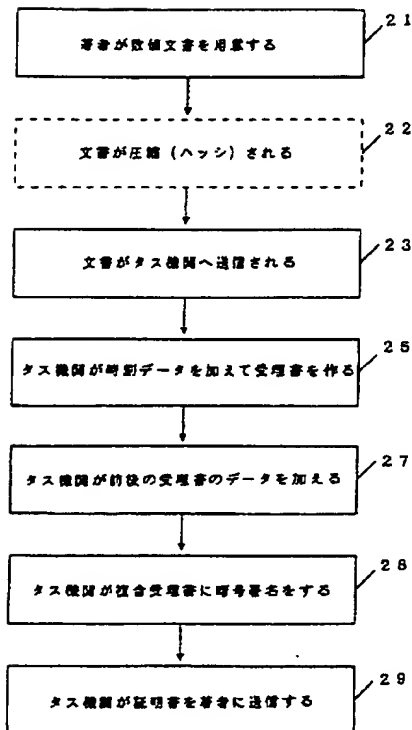
第5図に叙述されているもっと一般的な記録連鎖の手順では、拡大するシリーズの文書が、

作られる度に、通関の中でまたはタス機関で、処理されます。段階51では、決定部でハッシュして作られるような、新しい文書の表示が得られ、段階52では、前の文書を処理して得られた受取部と通関されます。段階53では、この通関表示が処理され、すなわちハッシュされ、現在の文書に対する新しい通関値を作ります。この値は通関に記録され、証明書にすめられるか、あるいは単に通関系に保持されて段階54で表示される次の文書に適用されます。以後の処理段階55、56はこの文書表示に適用され、この手順は新しい文書が来る度に繰り返されます。

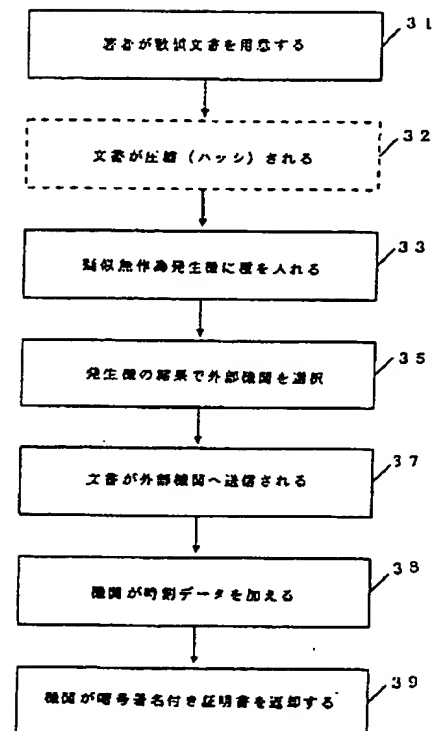
特表平6-501571 (8)



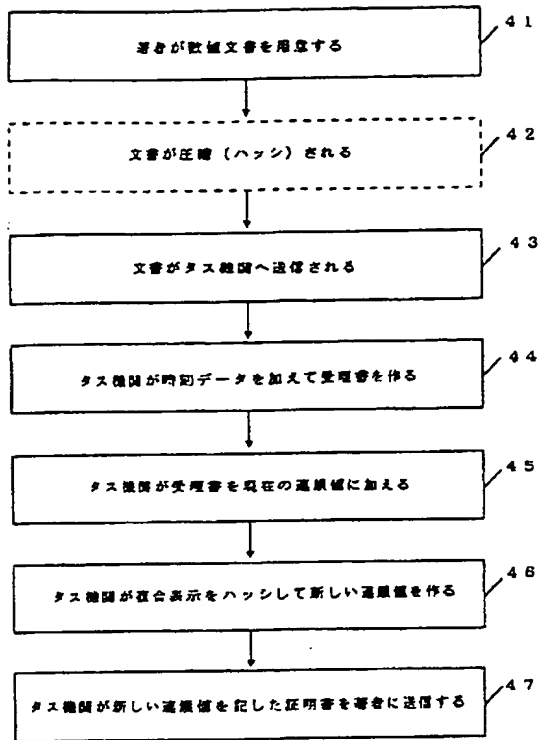
第1図



第2図

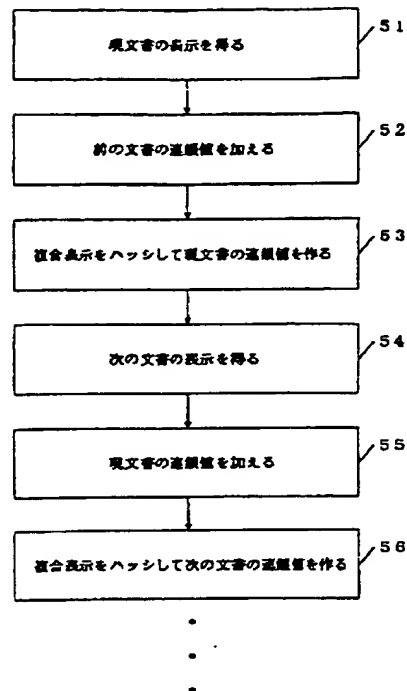


第3図



第 4 図

特表平6-501571 (9)



第 5 図

国際調査報告

Document submitted by *Dr. J. P. ...*

1. CLASSIFICATION OF SUBJECT MATTER Referring to International Patent Classification (IPC) or to other material Classification and I.P.D. Int. Cl.: <i>H01L 9/00</i> U.S. Cl.: <i>302/49</i>		
2. FIELD SEARCHED U.S. <i>302/4, 31, 32, 40, 50</i>		
3. DOCUMENTS CITED A <i>US, A, 4,145,565 PUBLISHED 20 MARCH 1979, DRAKE</i> 1-15 A <i>US, A, 4,128,315 PUBLISHED 03 JUNE 1978, POTAS ET AL.</i> 1-15		
4. SUMMARY OF INVENTION (a) <i>...</i> (b) <i>...</i> (c) <i>...</i> (d) <i>...</i> (e) <i>...</i> (f) <i>...</i> (g) <i>...</i> (h) <i>...</i> (i) <i>...</i> (j) <i>...</i> (k) <i>...</i> (l) <i>...</i> (m) <i>...</i> (n) <i>...</i> (o) <i>...</i> (p) <i>...</i> (q) <i>...</i> (r) <i>...</i> (s) <i>...</i> (t) <i>...</i> (u) <i>...</i> (v) <i>...</i> (w) <i>...</i> (x) <i>...</i> (y) <i>...</i> (z) <i>...</i>		
5. STATE OF DISCLOSURE (a) <i>...</i> (b) <i>...</i> (c) <i>...</i> (d) <i>...</i> (e) <i>...</i> (f) <i>...</i> (g) <i>...</i> (h) <i>...</i> (i) <i>...</i> (j) <i>...</i> (k) <i>...</i> (l) <i>...</i> (m) <i>...</i> (n) <i>...</i> (o) <i>...</i> (p) <i>...</i> (q) <i>...</i> (r) <i>...</i> (s) <i>...</i> (t) <i>...</i> (u) <i>...</i> (v) <i>...</i> (w) <i>...</i> (x) <i>...</i> (y) <i>...</i> (z) <i>...</i>		
6. DATE OF DISCLOSURE 3 OCTOBER 1991		
7. DATE OF REPORT 22 NOV 1991		
8. NAME OF REPORTING AGENCY INTERNATIONAL PATENT OFFICE		
9. NAME OF REPORTING AGENCY INTERNATIONAL PATENT OFFICE		
10. NAME OF REPORTING AGENCY INTERNATIONAL PATENT OFFICE		

フロントページの続き

(81) 指定国 EP (AT, BE, CH, DE, DK, ES, FR, GB, GR, IT, LU, NL, SE), CA, JP

(72) 発明者 ストーンネット、ウェイクフィールド、スコット、ジュニア
アメリカ合衆国、07960 ニュージャージー州、モリスタウン、ハーディング テラス 34